IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA
WINSTON-SALEM DIVISION

NATALIE WELLS-REYES, *on behalf of herself and all others similarly situated*, Plaintiff, v. NOVANT HEALTH, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Natalie Wells-Reyes ("Plaintiff") brings this Class Action Complaint against Defendant, Novant Health, Inc. ("Novant Health" or "Defendant"), in her individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, her counsel's investigation, and upon information and belief as to all other matters, as follows:

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") and personal health information ("PHI")[1] including, but not limited to, demographic information such as email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning on Defendant's website; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes on Defendant's website.[2]

[1] This information is collectively referred to as "PII and PHI" or "Private Information."

[2] https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx (last visited August 21, 2022).

2. Defendant is a three-state integrated network of physician clinics, outpatient centers and hospitals. Its network consists of more than 1,800 physicians and 35,000 employees at more than 800 locations, including 15 medical centers and hundreds of outpatient facilities and physician clinics.[3]

3. Headquartered in Winston-Salem, North Carolina, Defendant serves more than 5 million patients annually.[4]

4. In May 2020, Defendant launched a promotional campaign to connect more patients to Defendant's MyChart patient portal, with the goal of improving access to care through virtual visits and provide increased accessibility to counter the limitations of in-person care.[5] Defendant's campaign involved Facebook advertisements and a Meta (Facebook parent company) tracking pixel placed on Defendant's health website to understand the success of those efforts on Facebook. A pixel is a piece of code that organizations commonly use to measure activity and experiences on their website.[6] In this case, the pixel was configured incorrectly and allowed private information to be transmitted from Defendant's website to Meta from Defendant's Health website and MyChart portal (the "Disclosure").[7]

5. Defendant discovered on June 17, 2022, that this Disclosure took place.[8]

6. Plaintiff provided Private Information to Defendant in order to receive services rendered and on the reasonable expectation that Defendant would protect her Private Information.

---

[3] https://www.novanthealth.org/Portals/92/novant_health/documents/media/2022_Media_kits/2022_Novant%20Health%20Fact%20Sheet_final.pdf (last visited August 21, 2022).
[4] *Id.*
[5] *See supra,* n.2.
[6] *Id.*
[7] *Id.*
[8] *Id.*

7. Despite the Disclosure taking place in June 2021, Defendant hid the Disclosure from its customers until August 12, 2022, when it sent letters to Disclosure victims (the "Notice Letter"). As a result, Plaintiff and Class members were not properly informed that their Private Information has been disclosed.

8. Indeed, Defendant has only now just started notifying Plaintiff and Class members about the Disclosure, meaning their information may have been exposed for several months before Defendant warned them. The number of patients affected has swelled to over 1,300,000.

9. Defendant's Notice Letter admits that Defendant disclosed Plaintiff and Class members' Private Information, including, but not limited to, demographic information such as email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning on Defendant's website; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes on Defendant's website.[9]

10. As a result of the Disclosure, Plaintiff and over one million Class members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the disclosure and the substantial and imminent risk of identity theft.

11. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

12. The exposed Private Information of Plaintiff and Class members can—and likely will—be sold on the dark web. Third parties can often offer for sale the unencrypted, unredacted

[9] *Id*.

Private Information to criminals. Plaintiff and Class members now face a lifetime risk of identity theft.

13. This Private Information was compromised due to Defendant's acts and omissions and the failure to protect the Private Information of Plaintiff and Class members. In addition to Defendant's failure to prevent the Disclosure, after discovering the breach, Defendant waited several months to report it to government agencies and affected individuals.

14. As a result of this delayed response, Plaintiff and Class members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

15. Plaintiff bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class members; (ii) warn Plaintiff and Class members of Defendant's inadequate information security practices; (iii) effectively secure software and/or hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents; and (iv) utilize the correct pixel settings to prevent unlawful disclosure of Plaintiff's and Class members' Private Information. Defendant's conduct violates federal and state statutes.

16. Plaintiff and Class members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Disclosure, including but not

limited to lost time, and (iv) the continued and substantially increased risk to their Private Information which: (a) may remain unencrypted and/or in the wrong pixel configuration and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

17. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the Private Information of Plaintiff and Class members was compromised through disclosure to an unauthorized third party. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

18. Moreover, Defendant's negligence has affected over one million Class members all across the country. Indeed, according to its report submitted the United States Department of Health and Human Services, Defendant admits that the Private Information of 1,362,296 individuals was disclosed.[10]

PARTIES

19. Plaintiff Natalie Wells-Reyes is a resident and citizen of the State of North Carolina.

[10] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Aug. 22, 2022).

20. Plaintiff received a Notice Letter dated August 12, 2022 from Defendant Novant Health. The Notice Letter stated that in May 2020, a tracking pixel was placed on Defendant's website to help it to understand the success of its advertisement efforts on Facebook. A pixel is a piece of code that organizations commonly used to measure activity and experiences on their websites. In this case, the pixel was placed on Defendant's website to help it understand the success of campaign efforts on Facebook to get more patients connected to the Novant Health MyChart patient portal. In the Notice Letter, Novant Health states, "the pixel was configured incorrectly, and may have allowed certain private information to be transmitted to Meta (also known as Facebook) from the Novant Health website and MyChart portal."

21. The information sent from Defendant Novant Health's website and patient portal to Facebook included Protected Health Information ("PHI") as defined under the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 ("HIPAA").

22. In the Notice Letter, Defendant Novant Health claims it disabled the Facebook ad upon learning it had the capacity to transmit PHI and other Private Information to Meta, yet it does not specify when it learned of this capacity.

23. The PHI and other sensitive information sent by Defendant Novant Health to Facebook included, but was not limited to:

- Email addresses;
- Phone numbers;
- Computer IP addresses;
- Contact information entered into Emergency Contacts or Advanced Care Planning; and
- Information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes.

24. The Notice Letter from Defendant Novant Health further states that Plaintiff logged into the patient portal during the period from May 2020 until the undisclosed date that Defendant discovered the pixel's capacity to transmit Private Information to Meta. Plaintiff first logged onto Defendant's MyChart portal in approximately June of 2020.

25. Defendant Novant Health, Inc. is a North Carolina company with its principal place of business at 2085 Frontis Plaza Boulevard, Winston-Salem, North Carolina 27103.

JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

27. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

28. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATION

Defendant Disclosed Plaintiff's and Class Members' Private Information

29. In May 2020, Defendant launched a promotional campaign to connect Plaintiff and Class members to Defendant's MyChart patient portal, with the goal of improving access to care through virtual visits and provide increased accessibility.[11]

[11] *See supra,* n.2.

30. Defendant's campaign involved Facebook advertisements and a Meta (Facebook parent company) tracking pixel placed on Defendant's website to assist Defendant in understanding the results of its marketing efforts on Facebook.[12] A tracking pixel is a piece of code that organization commonly used to measure activity and experiences on their website.[13]

31. By seeking Defendant's services as a medical provider, Plaintiff and Class members unknowingly subjected their Private Information to the tracking pixel placed on Defendant's website.

32. Specifically, through Defendant's website, Plaintiff and Class members submitted Private Information that they did not intend to, nor had any reason to suspect would, be tracked by Facebook.

33. Defendant then used Plaintiff's and Class members' website submissions to track the effectiveness of its Facebook marketing campaign.

34. Defendant did not disclose to Plaintiff or Class members that Defendant used Plaintiff's and Class members' communications on its website and MyChart patient portal for marketing purposes.

35. Defendant tracked Plaintiff's and Class members' Private Information via the tracking pixel from May 2020 to June 17, 2022.

36. On or around June 17, 2022, it was discovered that Defendant's tracking pixel was configured incorrectly, and in turn, transmitted Plaintiff's and Class members' Private Information to Facebook and (its parent company) Meta.

37. Plaintiff and Class members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information.

[12] *Id*.
[13] *Id*.

38. By law, Plaintiff and Class members are entitled to privacy in their protected health information and confidential communications. Defendant deprived Plaintiff and Class members of their privacy rights when it: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook—an unauthorized third-party eavesdropper; and (3) undertook this pattern of conduct without notifying Plaintiff and Class members and without obtaining their express written consent.

Facebook's Platform and its Business Tools

39. Facebook describes itself as a "real identity platform,"[14] meaning users are allowed only one account and must share "the name they go by in everyday life."[15] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[16]

40. In 2021, Facebook generated $117 billion in revenue.[17] Roughly 97% of that came from selling advertising space.[18]

41. Facebook sells advertising space by highlighting its ability to target users.[19] Facebook can target users so effectively because it surveils user activity both on and off its site.[20]

---

[14] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).
[15] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.
[16] FACEBOOK, SIGN UP, https://www.facebook.com/.
[17] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx.
[18] *Id.*
[19] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706.
[20] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[21] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[22]

42. Advertisers can also build "Custom Audiences."[23] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[24] With Custom Audiences, advertisers can target existing customers directly, and they can also build a "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[25] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools."[26]

---

[21] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[22] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.

[23] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.

[24] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[25] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328.

[26] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.

43. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[27] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

44. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[28] Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[29] Advertisers can even create their own tracking parameters by building a "custom event."[30]

45. One such Business Tool is the Facebook Tracking Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their website. As the name implies, the Facebook Pixel "tracks the people and type of actions they take."[31] When a user accesses a website

---

[27] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.

[28] *See* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[29] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

[30] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[31] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

hosting the Facebook Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's websites—Defendant's own code, and Facebook's embedded code.

46. An example illustrates the point. Take an individual who navigates to Defendant's website and clicks on a tab for allergy information. When that tab is clicked, the individual's browser sends a GET request to Defendant's server requesting that server to load the particular webpage. Because Novant Health utilizes the Facebook Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual that this is happening. Facebook causes the browser to secretly duplicate the communication with Novant Health, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

47. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

Defendant's Privacy Policy[32]

48. Defendant's privacy policy states, "We must protect the privacy of health information about you that can identify you."[33]

[32]https://www.novanthealth.org/Portals/92/Assets/Documents/Corporate/PDFs/Novant%20Health%20Notice%20of%20Privacy%20Policies%20for%20North%20Carolina.pdf (last visited August 22, 2022).
[33] *Id*.

49. The privacy policy explains Defendant's legal duties with respect to Private Information and the exceptions for when Defendant can lawfully use and disclose Plaintiff's and Class members' Private Information in the following ways:

- To provide healthcare treatment to you;
- To obtain payment for services;
- For healthcare operations;
- To raise money for our organization;
- To remind you about appointments;
- To tell you about treatment options;
- To our business associates;
- When it is required by law;
- For public health activities;
- For health oversight activities;
- For a legal proceeding;
- For law enforcement purposes;
- To a medical examiner or funeral director;
- For organ, eye, or tissue donation purposes;
- For medical research;
- To avoid a serious threat to health or safety;
- For specialized government functions; and
- For law enforcement custodial situations.

50. Defendant's privacy policy does not permit Defendant to use and disclose Plaintiff's and Class members' Private Information for marketing purposes.

51. Defendant violated its own privacy policy by unlawfully disclosing Plaintiff's and Class members' Private Information to Facebook and Meta.

Plaintiff Natalie Wells-Reyes's Experience

52. Plaintiff sent to Defendant via its website and/or MyChart patient portal and allowed Defendant to store her health care records with her most intimate health care and financial information in its patient portal because she believed her PHI and other Personal Information would be protected as the law requires. Defendant did not protect her PHI and other personal information. Instead, upon information and belief, Defendant sent her PHI and other Personal Information to Facebook.

53. Plaintiff greatly values her privacy, PHI, and other Personal Information, especially in the health care setting where privacy should be at its greatest. Prior to the Disclosure, Plaintiff took reasonable steps to maintain the confidentiality of her PHI and other Personal Information.

54. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff faces, Defendant claimed it took the Disclosure very seriously, disabled the pixel, and implemented more structure, governance, and policies around the use of pixels from their site, and that it would take appropriate actions to ensure such a Disclosure did not happen again. Defendant claimed it did not have evidence that Facebook acted on the PHI and other sensitive information it received, but it invited Plaintiff to access links provide by Defendant. However, Plaintiff has not visited the links provided, as she does not trust Defendant to protect her information. In the letter, Defendant did not offer to pay for identity protection or credit monitoring.

55. Since learning of the Disclosure, Plaintiff has spent additional time reviewing her bank statements and credit cards.

56. Plaintiff has experienced an increase of spam calls, text messages and emails after the Disclosure.

57. As a result of this Disclosure leading to an increase in spam calls and text messages, Plaintiff has had substantial interference with her work and family life due to the time spent handling the fallout from this Disclosure.

58. The Disclosure has caused Plaintiff to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Defendant has not been forthright with information about the Disclosure.

59. Plaintiff plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Disclosure, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

60. Additionally, Plaintiff is very careful about sharing her PHI and other Personal Information. She has never knowingly transmitted unencrypted PHI over the internet or any other unsecured source.

61. Plaintiff has a continuing interest in ensuring that Defendant protects and safeguards her PHI and other Personal Information, which, upon information and belief, remains in Defendant's possession.

CLASS ACTION ALLEGATIONS

62. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated (the "Class") pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

63. The nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the United States whose Private Information was compromised in the Disclosure affecting Defendant, including all persons to whom Defendant sent notice about the Disclosure.

64. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, Defendant's officers, directors, successors and assigns, and any Judge who adjudicates this case, including his or her staff and immediate family.

65. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

66. Numerosity, Fed R. Civ. P. 23(a)(1): The Class members are so numerous that joinder of all members is impracticable. Upon information and belief, there are over one million individuals whose PII and PHI may have been improperly accessed in the Disclosure, and the Class is identifiable within Defendant's records.

67. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class members;

b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendant violated its privacy policy by disclosing the PII and PHI of Plaintiff and Class members to Facebook and Meta;

d. Whether and when Defendant actually learned of the Disclosure;

e. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their PII and PHI had been compromised;

f. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class members that their PII and PHI had been compromised;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Disclosure to occur;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class members;

i. Whether Defendant violated the laws invoked herein;

j. Whether Plaintiff and Class members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Defendant knowingly made false representations as to it data security and/or privacy policy practices;

l. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices;

m. Whether Plaintiff and Class members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Disclosure.

68. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class members because all had their PII and PHI compromised as a result of the Disclosure, due to Defendant's misfeasance.

69. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class members. Plaintiff has also retained counsel experienced in complex class actions, and Plaintiff intends to prosecute this action vigorously.

70. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

71. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

72. The nature of this action and the nature of laws available to Plaintiff and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

73. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

74. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII and PHI of Class members, Defendant may continue to refuse to provide proper notification to Class members regarding the Disclosure, and Defendant may continue to act unlawfully as set forth in this Complaint.

75. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

76. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class members' Private Information;

b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class members' Private Information with respect to Defendant's privacy policy;

c. Whether Defendant breached a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendant adequately and accurately informed Plaintiff and Class members that their Private Information had been compromised;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Disclosure;

g. Whether Class members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

///

///

COUNT I

VIOLATION OF THE WIRETAP ACT
18 U.S.C. § 2510, *et seq.*
(On Behalf of Plaintiff and the Class)

77. Plaintiff re-alleges and incorporates by reference paragraphs 1-76 in the Complaint as if fully set forth herein.

78. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents of any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

79. The Wiretap Act protects both the sending and receipt of communications.

80. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

81. Defendant is an electronic communications service as defined by 18 U.S.C. § 2510(15). Defendant intentionally divulged the contents of Plaintiff's and Class members' communications to Facebook wile in transmission. Defendant violated 18 U.S.C. § 1522(3)(a), which provides that an "entity providing an electronic communication service to te public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."

82. Defendant's actions in divulging the contents of Plaintiff's and Class members' communications to Facebook was intentional as shown by the intentional act of Defendant placing Facebook's pixel on its website and MyChart patient portal.

83. Defendant's conduct in divulging the content of communications and/or assisting Facebook's interception of Internet communications that Plaintiff and Class members were sending and receiving was done contemporaneously with Plaintiff's and Class members' sending and receipt of those communications and was done without Plaintiff's or Class members' authorization. In fact, Defendant's conduct ensured that Facebook received the communications before the communications between the Plaintiff or Class members and Defendant's website were completed.

84. The communications which Defendant intentionally divulged to and/or allowed to be intercepted by Facebook included "contents" of electronic communications made from Plaintiff and Class members to Defendant's website and patient portal in the form of PHI and PII which Plaintiff and Class members entrusted to Defendant and for which Plaintiff and Class members received communications in return from that website and patient portal.

85. The transmission of data between Plaintiff and the Defendant's website and patient portal, which Defendant divulged to and/or allowed to be intercepted by Facebook without Plaintiff's authorization, were "transfer[s] of signs, signals, writing, … data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, or photo-optical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

86. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The pixel Defendant placed on its website which allowed Facebook to track Plaintiff's communications while she used Defendant's website;

b. The Plaintiff's browsers;

c. The Plaintiff's computing devices;

d. Defendant's and Facebook's web servers;

e. The computer code deployed by Defendant which was received from Facebook to effectuate its tracking and interception of the Plaintiff's communications; and

f. The plan Defendant participated in with Facebook and carried out to effectuate Facebook's tracking and interception of Plaintiff's communications.

87. Facebook was not an authorized party to the communication because Plaintiff and Class members: i) were unaware of Defendant's placement of the pixel which redirected the communications to Facebook; and ii) did not knowingly send the communications to Facebook. Facebook could not manufacture its own status as a party to the Plaintiff's communications with Defendant by surreptitiously redirecting or intercepting those communications. Defendant cannot singlehandedly grant Facebook consent to intercept Plaintiff's communications. Defendant holds responsibility for its actions in placing the pixel on its website as an intercept device and divulging communications to Facebook and/or allowing Facebook to surreptitiously intercept those communications.

88. As illustrated herein, "the" communications between the Plaintiff and Defendant's website were simultaneous with, but separate from, the acquisition of the contents of those communications by Facebook.

89. Plaintiff did not consent to Facebook's interception of her communications while she was performing searches and communicating with Defendant on Defendant's website and patient portal. Defendant explicitly promised Plaintiff that it would not share her PII and PHI with others without her consent or for marketing purposes.

90. Through the complicity of Defendant in disclosing and/or facilitating the interception of the communications, Facebook, upon information and belief, then used the contents

of the PII and PHI knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

91. As a result of the above actions and pursuant to 18 U.S.C. § 2520, Plaintiff, on behalf of herself and the Class, seeks statutory damages; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future; and reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT II

INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

92. Plaintiff re-alleges and incorporates by reference paragraphs 1-76 in the Complaint as if fully set forth herein.

93. Plaintiff and Class members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

94. Defendant owed a duty to Plaintiff and Class members to keep their Private Information confidential.

95. The unauthorized disclosure to and/or acquisition (*i.e.,* theft) by a third party of Plaintiff's and Class members' Private Information is highly offensive to a reasonable person.

96. Defendant's reckless and negligent failure to protect Plaintiff's and Class members' Private Information constitutes an intentional interference with Plaintiff's and the Class members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

97. Defendant acted with a knowing state of mind when it permitted the Disclosure because it knew its information security practices were inadequate.

98. Defendant knowingly did not notify Plaintiff and Class members in a timely fashion about the Disclosure.

99. Because Defendant failed to properly safeguard Plaintiff's and Class members' Private Information, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class members.

100. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiff and the Class members was disclosed to and/or stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

101. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant with its inadequate cybersecurity system and policies.

102. Plaintiff and Class members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiff and the Class.

103. Plaintiff, on behalf of herself and Class members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class members' Private Information.

104. Plaintiff, on behalf of herself and Class members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by

Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT III

VIOLATION OF NORTH CAROLINA'S UNFAIR AND DECEPTIVE TRADE PRACTICE ACT
N.C. Gen. Stat. § 75-1.1, *et seq*.
(On behalf of Plaintiff and the Class)

105. Plaintiff re-alleges and incorporates by reference paragraphs 1-76 in the Complaint as if fully set forth herein.

106. N.C. Gen. Stat. § 75-1.1. (the "NC UDTPA") declares unlawful "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."

107. Defendant's conduct was in and affecting commerce and constitutes an unfair or deceptive trade practice under the NC UDPTA.

108. Specifically, Defendant's unlawful disclosure of Plaintiff's and Class members' Private Information constitutes a per se violation of NC UDPTA.

109. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of its services in violation of the NC UDPTA by: (i) unlawfully disclosing Plaintiff's and Class members' Private Information to Facebook; (ii) failing to disclose or omitting material facts to Plaintiff and Class members regarding the disclosure of their Private Information to Facebook; and (iii) failing to take proper action to ensure the pixel was configured to prevent unlawful disclosure of Plaintiff's and Class members' Private Information.

///

///

110. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant knew it failed to disclose to Plaintiff and Class members that their website submissions would be disclosed to Facebook.

111. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant intended that Plaintiff and Class members rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of services.

112. In addition, Defendant's material failure to disclose that Defendant collects Plaintiff's and Class members' Private Information for marketing purposes with Facebook constitutes an unfair act or practice prohibited by the NC UDPTA. Defendant's actions were immoral, unethical, and unscrupulous.

113. Defendant willfully, knowingly, intentionally, and voluntarily engaged in the aforementioned acts.

114. As a result of Defendant's wrongful conduct, Plaintiff and the Class were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their Private Information from being disclosed, taken and misused by others.

115. As a direct and proximate result of Defendant's violations of the NC UDPTA, Plaintiff and Class member have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiff and Class members would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII and PHI; and harm

resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

116. Pursuant to N.C. Gen. Stat. § 75-16, § 75.16.1, Plaintiff requests damages, treble damages, and attorneys' fees.

COUNT IV

BREACH OF CONFIDENCE
(On behalf of Plaintiff and the Putative Class)

117. Plaintiff re-alleges and incorporates by reference paragraphs 1-76 in the Complaint as if fully set forth herein.

118. In North Carolina, medical providers have a duty to their patients to keep non-public medical information completely confidential.

119. Plaintiff has reasonable expectations of privacy in her communications exchange with Defendant, including communications exchanged on Defendant's website and on the log-in page for Defendant's MyChart portal.

120. Plaintiff's reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its privacy policy.

121. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed pixel code to disclose and transmit Plaintiff's personally identifiable, non-public medical information, and the contents of their communications exchanged with Defendant to third parties.

122. The third-party recipients included, but were not limited to, Facebook and Meta.

123. Defendant's disclosures of Plaintiff's and Class members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

124. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

125. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the provider-patient relationship;

c. General damages for invasion of their rights in an amount to be determined by a jury;

d. Nominal damages for each independent violation;

e. Defendant took something of value from Plaintiff and Class members and derived benefit therefrom without Plaintiff's and Class members' knowledge or informed consent and without compensating Plaintiff for the data;

f. Plaintiff and Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

g. Defendant's actions diminished the value of Plaintiff's and Class members' Personal Information; and

h. Defendant's actions violated the property rights Plaintiff and Class members have in their Personal Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiff and her Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

a. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined at trial;

b. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

c. For prejudgment interest on all amounts awarded; and

d. Such other and further relief as this Court may deem just and proper.

///

///

///

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

DATED: September 22, 2022

Respectfully Submitted,

By, */s/Michael C. Wells*

R. Michael Wells, Jr. (NCSB: 33526)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
7 Corporate Center Court, Suite B
Greensboro, NC 27408
Telephone: (336) 970-3354
Facsimile: (916) 924-1829
Email: mwells@justice4you.com

M. Anderson Berry*
Gregory Haroutunian*
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
Email: aberry@justice4you.com;
gharoutunian@justice4you.com

Rachele R. Byrd*
Alex Tramontano*
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
Email: byrd@whafh.com; tramontano@whafh.com

**Pro hac vice forthcoming*

Counsel for Plaintiff and the Class